

-
- [News](#)
 - [News & Analysis](#)
 - [Press Releases](#)
- [Interviews](#)
- [CIO](#)
 - [CIO Life](#)
 - [CIO Blogs](#)
 - [Perspective](#)
 - [Global CIO](#)
- [Resources](#)
 - [Whitepapers](#)
 - [Analytics & Reports](#)
 - [Print Magazine](#)
 - [Digital Issues](#)
- [Webcast](#)
 - [All Webcast](#)
 - [Upcoming Webcast](#)
 - [On demand Webcast](#)
 - [By Company](#)
- [Industries](#)
 - [BFSI](#)
 - [IT-ITeS](#)
 - [Government](#)
 - [FMCG](#)
 - [Telecom](#)
 - [Manufacturing](#)
 - [Healthcare](#)
 - [Education](#)
 - [Services](#)
- [Tech Center](#)
 - [IBM](#)
- More
 - [Case Studies](#)
 - [Slide Shows](#)
 - [Videos](#)
 - [FSA](#)
 - [EDGE](#)
 - [PR Newswire](#)
 - [Advertise with Us](#)
 - [Contact Us](#)
- [Login](#)
- [Register](#)



- [Security](#)
- [Software](#)
- [Storage](#)
- [Mobility](#)
- [Cloud Computing](#)
- [Big Data](#)
- [Social](#)
- [Virtualization](#)
- [Innovation and Action](#)
- [Internet](#)
- [BI/Analytics](#)
- More

Latest Stories:

[5 IT job interview mistakes new graduates make](#)

-
-
-

Follow Us :

- 
- 
- 
- 
- 
- 







- [Home](#)
- [News Analysis](#)
- [Software](#)

Software

The value of privacy in the age of Internet of Things

by Monica Rozenfeld, [IEEE](#), May 11, 2014

Will the The Internet of Things create a completely new scenario for privacy? Let's find out

-  1
-  6
-  0
-  4
- 
- 

More Insights

[Webcasts](#)

- [Intelligence-driven incident response for today's enterprise](#)
- [Migrating to the next gen secure enterprise mobility platform with Samsung](#)

[More](#)

[Downloads](#)

- [Enhance SAP Productivity with Magic xpi to Improve Business Performance.](#)
- [5 Keys to Preventing Advanced Attacks](#)
- [Controlling Advanced Persistent Threats Using the Next-Generation Firewall](#)

[More](#)

The Internet of Things promises many advances, such as the ability for consumers to keep track of their energy usage on their phones or receive alerts when milk is running low. Everything, including our homes and our heartbeats, will be monitored to make our lives easier and healthier.

But with the IoT, or what some call the “Internet of Everything,” companies are planning to turn information about our every move into valuable market data. Soon, personalized ads—like those that follow online users from one website to the next—are likely to follow us in text messages and on face-scanning screens as we walk down store aisles. Information such as the purchases we make, our genders and ages, and the places we frequent will be collected to inform us—whether we care to know or not—what we might want to buy next. Although some argue that this brings added value by personalizing the shopping experience, others believe such uses of the IoT are invasions of privacy.

“Privacy as we know it will have to be completely redefined,” says IEEE Senior Member Raul Colcher, CEO of Questera, an information technology consulting company in Rio de Janeiro. He advises businesses on how to handle privacy and security as the IoT evolves.

“The Internet of Things will create a completely new scenario for privacy and security that will need to be addressed,” Colcher says. He adds that we are already dealing with related issues, including companies collecting information about us from our online activity. But with the IoT, more of our information will be available. We’re likely to be sent reminders that, for example, we’re running low on shampoo or are overdue for a vacation.

The Future is here

Many IoT applications are already here. Sensor technology products for smarter homes, for example, can provide families with peace of mind, as their ads suggest. With just a click on a mobile device, users can activate a security system in a home, turn off lights while away on vacation, turn up the thermostat on a cold night while still an hour from

home, or lock the front door from the driveway. Signals from all those sensors travel through a wireless network to be stored in the cloud, with the information analyzed and acted upon. And that can sometimes be problematic.

“Who is controlling what’s in the cloud? Do I trust my cloud-computing system?” asks IEEE Senior Member Neeli Prasad, vice president at SAI Technology, a developer of mobile cloud network systems in Santa Clara, Calif. “Do I trust the people who have access to my information?”

If privacy is of great concern, individuals may have to become their own service providers, says Prasad. She sees a trend toward home cloud-computing systems in which individuals store their information privately instead of relying on companies. “That way, we can choose what information leaves our homes and becomes part of the public cloud and what doesn’t.”

Many new products on the market, including the video-streaming service Hulu and the Nike Fuelband, which monitors exercise activity, give consumers the option to sync those products with their social networks and mobile phones, essentially storing that information in cloud systems and databases. Thus, they can share information with the public about what TV shows they watch or how much they exercise. Or not. “Users can deny this option,” Prasad says. One example is the recent news that consumers will be able to opt out of Wi-Fi tracking that allows companies to collect information about the places people visit and the purchases they make through their smartphones.

Concern over unauthorized access to private information is not increasing, she says. There is just more of it to worry about. “Sometimes the shadow of a new technology and its applications are scarier than the thing itself,” she says. Moreover, not every application is intended to sell us something or observe our private lives. For example, law enforcement can track a missing person by accessing the GPS coordinates in a smartphone. (So can relatives and friends who have security access via a mobile app, such as Find My iPhone.)

A precautionary tale

Not all are as optimistic as Prasad about the future of the IoT. While users may have control over who in the general public sees their information, the bigger concern for consumer privacy expert Katherine Albrecht is the question of who owns the data. She is an executive with StartPage, a search engine that does not collect or share personal information, and StartMail, an encrypted e-mail service.

An article coauthored with IEEE Senior Member Katina Michael, “[Connected: To Everyone and Everything](#),” in the Winter 2013 issue of IEEE Technology and Society Magazine, puts Albrecht’s concern bluntly: “[Consumers] may think we’re in charge of our shopper cards and our mobile apps and our smart fridges—but ... let’s not fool ourselves. [The information] is not ours. It belongs to Google, and IBM, and Cisco Systems...and the global Mega-Corp that owns your local supermarket. If you don’t believe us, just try removing ‘your’ data from their databases.”







Michael is the associate dean international of the University of Wollongong Faculty of Engineering and Information Sciences, in Australia, and editor in chief of IEEE Technology and Society Magazine.

To prepare for the interconnected future, businesses and governments are outlining measures to be taken while new policies are developed. The European Union, for example, outlined such measures in its report “IoT Privacy, Data Protection, Information Security,” published in January 2013. One recommendation is to develop privacy-friendly default settings on IoT products and services that would give users more control over what information is shared with others. Furthermore, it suggests that IoT networks give individuals the rights to their own data. In 2012, participants at the Open IoT Assembly—an initiative to envision a future with the IoT—developed an “IoT Bill of Rights” at a two-day conference in London that calls for transparency of IoT processes and the preservation of privacy. It also calls for people to have access to their personal data.

Despite potential risks to privacy, companies are betting their customers will see the advantages that the IoT will bring them, says Colcher. But some groups advocate that consumers have the power to slow down or even stop the advancement of the IoT. Not Colcher. “The inclusion of the IoT all around us is inevitable,” he says. “The only thing to

do now is to prepare the best we can.”

Source: [IEEE](#)

-  0
-  6
-  0
-  3
- 
- 

• Tags: [IEEE](#), [Internet of Things](#), [Privacy](#), [IoT](#)

0 Comments

InformationWeek India

 Login ▾

Sort by Newest ▾

Share  Favorite 



Start the discussion...

Be the first to comment.

ALSO ON INFORMATIONWEEK INDIA

WHAT'S THIS?

Mark Zuckerberg explains why Facebook acquired WhatsApp - InformationWeek ...

1 comment • 3 months ago



Viraj Mehta — This is why Mark and Facebook acquired WhatsApp

Security as a Service: Evolutionary or revolutionary? - InformationWeek – IT ...

1 comment • 2 months ago



Eddie Mayan — Yes, security concerns even many providers like cloudways offer free consultancy on cloud security for ...

How Mindtree's holistic focus on saving energy is yielding great results

1 comment • 7 days ago



Parvez Ansari — We all should take advantage of Mindtree's experience and follow the footsteps of them in order to ...

Opportunities galore for smartwatch makers - InformationWeek – IT news & ...

2 comments • 2 months ago



Andrew Till — Hi Shrikant, thanks for the comments it's always good to start a debate. As you ask actually yes I have as ...

 Subscribe

 Add Disqus to your site

Popular News



[Internet](#)

[The Internet of Things is moving to the mainstream](#)



[Software](#)

['We want to leverage technology for society': CN Raghupathi, Head, Infosys India Business Unit...](#)

[Security](#)

[India ranks #7 in the number of computers compromised by banking Trojans in 2013](#)

Subscribe for Newsletter

Stay connected to the best business technology content every week. Subscribe to our daily newsletter now!

Email Address

Polls

What is your preferred Smartphone

- ☐ Apple iPhone
- ☐ Samsung Galaxy S4
- ☐ Blackberry Z10

Related Stories

- [IoT security requirements will reshape over half of global enterprise IT security programs by 2020: Gartner](#)
- [Rapid growth of the Internet of Things will add economic value: Gartner](#)
- [By 2020, Internet of Things will expand to 26 billion units and create new challenges for the Data center, says Gartner](#)
- [India needs to take on the Internet of Things](#)

More Software

- [5 IT job interview mistakes new graduates make](#)
- [Over 25 Indian startups to visit Silicon Valley courtesy NASSCOM 10,000 Start-ups program](#)
- [The rise of the digital enterprise](#)
- [Evalueserve taps into IBM to build private cloud environment for global knowledge centers](#)
- [Can Indian banks do a Flipkart in customer service?](#)

Whitepapers



- [Enhance SAP Productivity with Magic xpi to Improve Business Performance.](#) by [Magic Software Enterprises](#)



- [5 Keys to Preventing Advanced Attacks](#)



- [Controlling Advanced Persistent Threats Using the Next-Generation Firewall](#) by [Palo Alto Networks](#)

[More](#)



[Download Today](#)

Print Magazine

[April 2014](#)

- [Download Digital Issue](#)
- [View past issues](#)

Analytics & Reports

- [Voke Research: Market Snapshot Report - Service Virtualization](#)
- [Coleman Parkes Study: Business Benefits of Service Virtualization](#)
- [Taking the giant leap](#)

[More](#)

Slide Shows



[InformationWeek EDGE Award 2013...](#)

The winners of EDGE Awards 2013 were recently honored at a ceremony held at Leela Palace, Mumbai

Digital Issue



-

[Dysfunction Junction: A Pragmatic Guide to Getting Started with DevOps](#)



-

[The Cloud Handbook](#)



-

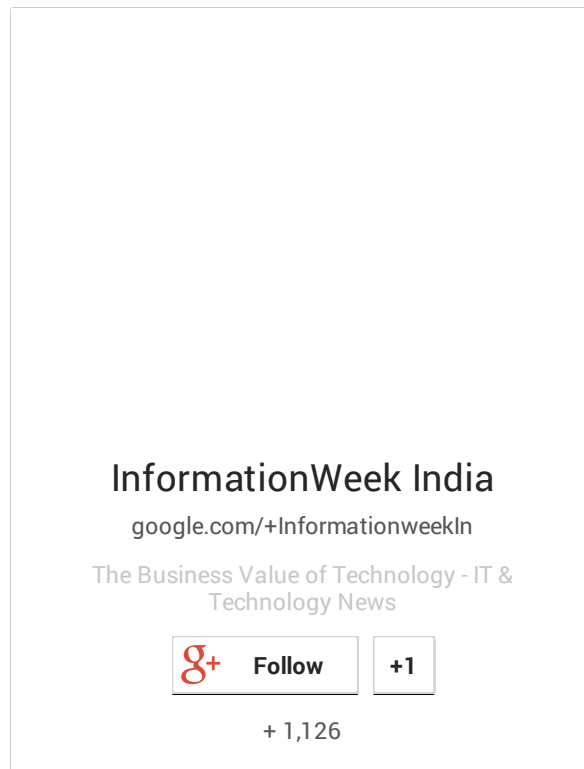
[Best of Security 2013](#)

[More](#)

Upcoming Demand Webcast

[Intelligence-driven incident response for today's enterprise](#)

RSA's Critical Incident Response Solution (CIRS) integrates the key elements for incident response capability that is intelligence-driven and risk-focused. CRIS incorporates a variety of integrated security tools that provide for security operations management. Attend this webcast and you get a closer look at how RSA's Critical Incident Response Solution (CIRS) integrates the key elements to give your organization an effective and efficient incident response capability. Date: 14 May, 2014 Time: 3:00-4:00pm



- [News & Analysis](#)
- [Perspective](#)
- [Interviews](#)
- [Case Studies](#)
- [Slide Shows](#)
- [Whitepapers](#)
- [Events](#)
- [Webcast](#)
- [Analytics & Reports](#)
- [Digital Issues](#)
- [CIO Life](#)
- [CIO Blogs](#)
- [Videos](#)



MEDIA :

- [CRN](#)
- [EDN India](#)
- [InformationWeek](#)
- [Light Reading](#)
- [TechOnline India](#)

EVENTS :

- [4G World](#)
- [Bangladesh CIO Summit](#)
- [CloudConnect](#)
- [CRN CDRS](#)
- [CRN Leadership Summit](#)
- [ESC](#)
- [FTS](#)
- [ICSC](#)
- [INTEROP](#)
- [Srilanka CIO Summit](#)
- [TFM&A India](#)

AWARDS :

- [CRN CDRS Awards](#)
- [CRN Xcellence Awards](#)
- [InformationWeek EDGE Awards](#)
- [InformationWeek Future Strategist Award](#)
- [InformationWeek Global CIO](#)

OTHERS :

- [CRN Channel Champions](#)

Copyright © 2013 UBM India, All rights reserved

- [Advertising Contacts](#)
- [About Us](#)
- [Privacy Statement](#)
- [Corporate Website](#)
- [Contact Us](#)